UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

Tabitha Baker on behalf of herself and all others similarly situated,	)	
Plaintiff,	)	CLASS ACTION
v.	)	CASE NO.
Yahoo, Inc., A Delaware Corporation	)	
Defendant.	)	JURY TRIAL DEMANDED

PLAINTIFF'S CLASS ACTION COMPLAINT

NOW COMES, the Plaintiff Tabitha Baker (hereinafter "Plaintiff"), by and through the undersigned counsel and files this Class Action Complaint against Defendant Yahoo, Inc. (hereinafter "Defendant") respectfully showing the Court as follows:

INTRODUCTION

1.

This action is brought to seek redress for damages sustained by Plaintiff and other members of the class as a result of the failure of Yahoo! Inc. (hereinafter referred to as "Yahoo" or "Defendant"), to securely store and maintain the personal information of Plaintiffs and the class.

2.

On December 14, 2016, Yahoo announced over 1,000,000,000 (One Billion) Yahoo users' account information was stolen by online hackers three years ago in August 2013. This includes names, email addresses, telephone numbers, birth dates, passwords, and security questions (referred to as "Personal Information" or "PI") of Yahoo account holders

3.

While investigating another potential data breach, Yahoo uncovered this data breach. Three years is unusually long period of time in which to identify a data breach. According to the Ponemon Institute, which tracks data breaches, the average time to identify an attack is 191 days and the average time to contain a breach is 58 days after discovery.

PARTIES AND SERVICE

4.

Plaintiff is a natural person and is the subject of the dispute complained about herein. Plaintiff is currently a resident of Fulton County, Georgia. Plaintiff has been a user of her yahoo account since in or around 1994 and a daily user since in or around 2010.

5.

Defendant Yahoo! Inc. is a Delaware corporation registered with the and is headquartered in Sunnyvale, California.

6.

This action is brought by Plaintiffs on behalf of a class comprising all similarly situated consumers nationwide.

7.

Defendant operates and markets its services throughout Georgia and the nation, which is within this judicial district.

JURISDICTION AND VENUE

8.

This Court has diversity jurisdiction over the action pursuant to 28 U.S.C. § 1332(d), because at least one class member is of diverse citizenship from Defendant and there are approximately 1 Billion class members nationwide. The aggregate amount in controversy exceeds five million dollars ($5,000,000.00), excluding interest and costs.

9.

Venue is proper in this district under 28 U.S.C. §1391 because Defendant engaged in substantial conduct relevant to Plaintiffs' claims within this District and have caused harm to class members residing within this district.

FACTUAL ALLEGATIONS

10.

Yahoo was founded in 1994 as a directory of web sites, but developed into a source for searches, email, shopping and news. Currently, its services still attract a billion visitors a month.

11.

Plaintiff and class members signed up for online Yahoo accounts that included providing personal information.

12.

On or about December 14, 2016, Yahoo informed its users that they were victims of a massive data breach, dating back to 2013. Yahoo said in a statement that "the account information may have included names, email addresses, telephone numbers, dates of birth, hashed passwords (the vast majority with bcrypt) and, in some cases, encrypted or unencrypted security questions and answers."

13.

Yahoo indicated that they believe a "state-sponsored actor" was behind the data breach, meaning an individual acting on behalf of a government. The breach is believed to have occurred in August 2013. It is estimated that at least

1 Billion user accounts have been stolen in what may be the largest data breach ever.

14.

The type of information compromised in this data breach is highly valuable to perpetrators of identity theft. Names, email addresses, telephone numbers, dates of birth, passwords and security question answers can all be used to gain access to a variety of existing accounts and websites.

15.

In addition to compromising existing accounts, the class members' PI can be used by identity thieves to open new financial accounts, incur charges in the name of class members, take out loans, clone credit and debit cards, and other unauthorized activities.

16.

Identity thieves can also use the PI to harm the class members through embarrassment, black mail or harassment in person or online. Additionally, they can use class members' personal information to commit other types of fraud including obtaining ID cards or driver's licenses, conducting immigration fraud, fraudulently obtaining tax returns and refunds, obtaining government benefits, evading arrest or citation by providing fraudulent information, and numerous others.

17.

The damage caused by identity theft in general registers in the billions of dollars.

18.

A Presidential Report on identity theft from 2008 states that:

> In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of nonfinancial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

The President's Identity Theft Task Force, Combating Identity Theft: A Strategic Plan, at p.11 (April 2007), available at <http://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theftstrategic-plan/strategicplan.pdf>.

19.

These problems are further exacerbated by the fact that many identity thieves will wait years before attempting to use the personal information they have

obtained. A Government Accountability Office ("GAO") study found that "stolen data may be held for up to a year or more before being used to commit identity theft." In order to protect themselves, class members will need to remain vigilant against unauthorized data use for years and decades to come. GAO, Report to Congressional Requesters, at p. 33 (June 2007), available at <www.gao.gov/new.items/d07737.pdf>

20.

Plaintiff and class members are at risk for identity theft in its myriad forms, potentially for the remainder of their lives.

CLASS ACTION ALLEGATIONS

21.

Plaintiffs bring this lawsuit on behalf of herself and as a class action, pursuant to Rules 23(a), (b)(2) and (b)(3) of the Federal Rules of Civil Procedure,

on behalf of a proposed class (the "Class"), defined as:

> All persons in the United States who were or are Yahoo account holders and whose personal or financial information was accessed, compromised, or stolen from Yahoo in 2013.

22.

Plaintiffs also bring this lawsuit on behalf of themselves and as a subclass, defined as:

> All persons in the State of Georgia who were or are Yahoo account holders and whose personal or financial information was accessed, compromised, or stolen from Yahoo in 2013.

23.

Excluded from the Class are Defendants and any entities in which Defendant or their subsidiaries or affiliates have a controlling interest, Defendant's officers, agents and employees, the judicial officer to whom this action is assigned and any member of the Court's staff and immediate families, as well as claims for personal injury, wrongful death, and emotional distress.

24.

Numerosity – Federal Rule of Civil Procedure 23(a)(1). The members of the Class are so numerous that joinder of all members would be impracticable. Plaintiffs reasonably believe that class members number approximately 500 million persons. As such, class members are so numerous that joinder of all members is impractical. The names and addresses of class members are identifiable through documents maintained by Yahoo.

25.

Commonality and Predominance – Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3). This action involves common questions of law or fact, which predominate over any questions affecting individual class members, including:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant owed a legal duty to Plaintiffs and the other class members to exercise due care in collecting, storing, and safeguarding their Personal Information;

c. Whether Defendant negligently or recklessly breached legal duties owed to Plaintiffs and the other class members to exercise due care in collecting, storing, and safeguarding their Personal Information and financial information;

d. Whether Defendant's conduct violated the Georgia Fair Business Practices Act of 1975

e. Whether Plaintiffs and the other class members are entitled to actual, statutory, or other forms of damages, and other monetary relief; and

f. Whether Plaintiffs and the other class members are entitled to

equitable relief, including, but not limited to, injunctive relief and restitution.

26.

Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs individually and on behalf of the other class members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

27.

Typicality – Federal Rule of Civil Procedure 23(a)(3). Plaintiffs' claims are typical of the claims of the other class members because, among other things, Plaintiffs and the other class members were injured though the substantially uniform misconduct described above. Plaintiffs herein are advancing the same claims and legal theories on behalf of themselves and all other class members, and there are no defenses that are unique to Plaintiffs.

28.

Adequacy of Representation – Federal Rule of Civil Procedure 23(a)(4). Plaintiffs are adequate representatives of the class because their interests do not conflict with the interests of the other class members they seek to represent;

they have retained counsel competent and experienced in complex class action litigation and Plaintiffs will prosecute this action vigorously. The class' interests will be fairly and adequately protected by Plaintiffs and their counsel.

29.

Superiority – Federal Rule of Civil Procedure 23(b)(3). A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiffs and the other class members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impracticable for class members to individually seek redress for Defendant's wrongful conduct. Even if class members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments, and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

30.

Application of Georgia law – Because Yahoo does business in the State of Georgia, Georgia law can and should apply to all claims relating to the data breach, even those made by persons who reside outside of Georgia.

CLAIMS ASSERTED

COUNT I

Violation of the Georgia Fair Business Practices Act of 1975

31.

Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in each and every paragraph above, as though fully stated herein.

32.

Defendant engaged in unfair, unlawful, and fraudulent business practices in violation of the GFBPA of 1975.

33.

By reason of the conduct alleged herein, Yahoo engaged in unlawful, unfair, and deceptive practices within the meaning of the ACT .

34.

Defendant stored Plaintiffs' and the other class members' PI in their electronic and consumer information databases. Yahoo represented to Plaintiffs and the other class members that its PI databases were secure and that customers'

PI would remain private. Yahoo engaged in deceptive acts and business practices by providing in its website that "protecting our systems and our users' information is paramount to ensuring Yahoo users enjoy a secure user experience and maintaining our users' trust." <https://policies.yahoo.com/us/en/yahoo/privacy/topics/security/index.htm>.

35.

Yahoo knew or should have known that it did not employ reasonable measures that would have kept Plaintiffs' and the other class members' PI and financial information secure and prevented the loss or misuse of Plaintiffs' and the other class members' PI and financial information.

36.

Yahoo's deceptive acts and business practices induced Plaintiffs and the other class members to use Yahoo's online services, and to provide PI. But for these deceptive acts and business practices, Plaintiffs and the other class members would not have provided their PI to Defendant.

37.

Yahoo's representations that it would secure and protect Plaintiffs' and the other class members' PI and financial information in its possession were facts that reasonable persons could be expected to rely upon when deciding whether to utilize Yahoo's services.

38.

Defendant violated the GFBPA of 1975 by misrepresenting the safety of their many systems and services, specifically the security thereof, and their ability to safely store Plaintiffs' and Class Members' PI. Yahoo also violated the UCL by failing to immediately notify Plaintiffs and the other Class members of the data breach. If Plaintiffs and the other Class members had been notified in an appropriate fashion, they could have taken precautions to safeguard their PI.

39.

Defendant's acts, omissions, and misrepresentations as alleged herein were unlawful and its own Privacy Policy.

40.

But for these deceptive acts and business practices, Plaintiffs and class members would not have purchased services from Yahoo or provided the required PI.

41.

Plaintiff and the other Class members suffered injury in fact and lost money or property as the result of Defendant's failure to secure Plaintiffs' and the other Class member's' PI contained in Defendant's servers or databases. As the result of the data breach, Plaintiff and other class members' personal information and financial information was compromised.

42,

Confidence in Defendant taking reasonable measures to protect Plaintiffs' and class members PI was a substantial factor in Plaintiffs' choosing to utilize Yahoo's online services.

43.

As a result of Defendant's violation, Plaintiffs and the other class members are entitled to restitution and injunctive relief.

COUNT II

NEGLIGENCE

44.

Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in each and every paragraph above, as though fully stated herein.

45.

Defendant owed a duty to Plaintiffs and the other class members to exercise reasonable care in safeguarding and protecting their PI and financial information in its possession from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing Defendant's security systems to ensure that Plaintiffs' and the other class members' PI and financial information was adequately secured and protected. Defendant further had a duty to implement

processes that would detect a breach of their security system in a timely manner.

46.

Defendant also had a duty to timely disclose to Plaintiffs and the other class members that their PI and financial information had been or was reasonably believed to have been compromised. Timely disclosure was appropriate so that, among other things, Plaintiffs and the other class members could take appropriate measures to cancel or change usernames, pin numbers, and passwords on compromised accounts, to begin monitoring their accounts for unauthorized access, to contact the credit bureaus to request freezes or place alerts, and take any and all other appropriate precautions.

47.

Defendant breached is duty to exercise reasonable care in safeguarding and protecting Plaintiffs' and the other class members' PI and financial information by failing to adopt, implement, and maintain adequate security measures to safeguard that information; allowing unauthorized access to Plaintiffs' and the other class members' PI and financial information stored by Defendant; and failing to recognize in a timely manner the breach.

48.

Defendant breached its duty to timely disclose that Plaintiffs' and the other class members' PI and financial information had been, or was reasonably

believed to have been, stolen or compromised.

49.

Defendant's failure to comply with industry regulations and the delay between the date of intrusion and the date Yahoo informed customers of the data breach further evidence Defendant's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and the other class members' PI and financial information.

50.

But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and the other class members, their PI and financial information would not have been compromised, stolen, and viewed by unauthorized persons.

51.

The injury and harm suffered by Plaintiffs and the other class members was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and the other class members' PI and financial information. Defendant knew or should have known that their systems and technologies for processing and securing Plaintiffs' and the other Class members' PI and financial information had security vulnerabilities.

82. As a result of Defendant's negligence, Plaintiffs and the other class members incurred economic damages relating to expenses for credit monitoring,

loss of use and value of their debit and/or credit cards, and loss of rewards on their debit and/or credit cards.

COUNT III

VIOLATION OF THE FEDERAL STORED

COMMUNICATIONS ACT, 18U.S.C. § 2702

52.

Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in each and every paragraph above, as though fully stated herein.

53.

The Federal Stored Communications Act ("SCA") contains provisions that provide consumers with redress if a company mishandles their electronically stored information. The SCA was designed, in relevant part, "to protect individuals' privacy interests in personal and proprietary information." S. Rep. No. 99-541, at 3 (1986), reprinted in 1986 U.S.C.C.A.N. 3555 at 3557.

54.

Section 2702(a)(1) of the SCA provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1).

55.

The SCA defines "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." Id. at § 2510(15).

56.

Through their equipment, Defendant provide an "electronic communication service to the public" within the meaning of the SCA because they provide consumers at large with mechanisms that enable them to send or receive wire or electronic communications concerning their private financial information to transaction managers, card companies, or banks.

57.

By failing to take commercially reasonable steps to safeguard sensitive private financial information, even after Defendant was aware that customers' PI and financial information had been compromised, Defendant knowingly divulged customers' private financial information that was communicated to financial institutions solely for customers' payment verification purposes, while in electronic storage in Defendant's payment system.

58.

Section 2702(a)(2)(A) of the SCA provides that "a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or

maintained on that service on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service." 18 U.S.C. § 2702(a)(2)(A).

59.

The SCA defines "remote computing service" as "the provision to the public of computer storage or processing services by means of an electronic communication system." 18 U.S.C. § 2711(2).

60.

An "electronic communications systems" is defined by the SCA as "any wire, radio, electromagnetic, photo-optical or photo-electronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." 18 U.S.C. § 2510(4).

61.

Defendant provides remote computing services to the public by virtue of its computer processing services for consumer credit and debit card payments, which are used by customers and carried out by means of an electronic communications system, namely the use of wire, electromagnetic, photo-optical or photo-electric facilities for the transmission of wire or electronic communications

received from, and on behalf of, the customer concerning customer private financial information.

62.

By failing to take commercially reasonable steps to safeguard sensitive private financial information, Defendant has knowingly divulged customers' private financial information that was carried and maintained on Defendant's remote computing service solely for the customer's payment verification purposes. As a result of Defendant's conduct described herein and their violations of Section 2702(a)(1) and (2)(A), Plaintiffs and the class members have suffered injuries, including lost money and the costs associated with the need for vigilant credit monitoring to protect against additional identity theft. Plaintiffs, on their own behalf and on behalf of the putative class, seeks an order awarding herself and the class the maximum statutory damages available under 18 U.S.C. § 2707 in addition to the cost for 3 years of credit monitoring services.

JURY TRIAL DEMANDED

63.

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury of all claims in this Consolidated Class Action Complaint so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other Class members, respectfully requests that this Court enter an Order:

A. Certifying the Class and the Subclass under Federal Rule of Civil Procedure 23(a), 23(b)(2) and (b)(3), appointing Plaintiffs as Class Representatives, and appointing their undersigned counsel as Class Counsel;

B. Finding that Defendant's conduct was negligent, deceptive, unfair, and unlawful as alleged herein;

C. Enjoining Defendant from engaging in the negligent, deceptive, unfair, and unlawful business practices alleged herein;

D. Awarding Plaintiffs and the other class members actual, compensatory, and consequential damages;

E. Awarding Plaintiffs and the other class members statutory damages;

F. Awarding Plaintiffs and the other class members restitution and disgorgement;

G. Requiring Defendant to provide appropriate credit monitoring services to Plaintiffs and the other class members;

H. Awarding Plaintiffs and the other class members pre-judgment and post-judgment interest;

I. Awarding Plaintiffs and the other class members reasonable attorneys' fees and costs, including expert witness fees; and

J. Granting such other relief as the Court deems just and proper.

Respectfully submitted this 14th day of December, 2016

/s/ Harlan S. Miller

Harlan S. Miller
Georgia Bar No. 506709
Miller Legal, P.C.
3646 Vineville Ave.
Macon, GA, 31204
(404) 931-6490
(478) 292-7808 (FAX)
hmiller@millerlegalpc.com

CERTIFICATE OF COMPLIANCE

This is to certify that the foregoing has been prepared using Times New Roman 14 point font.

This 14th day of December, 2016.

/s/ Harlan S. Miller
Harlan S. Miller
Georgia Bar No. 506709
hmiller@millerlegalpc.com